

CUANDO TODO TU DINERO VALE UN CARTÓN DE LECHE

Fake AP with legit passwords by
Dani Martínez - @danIt0

- danIt0@danIt0.com
- jmartinezcoronel@deloitte.es

CyberSOC Deloitte

INDICE

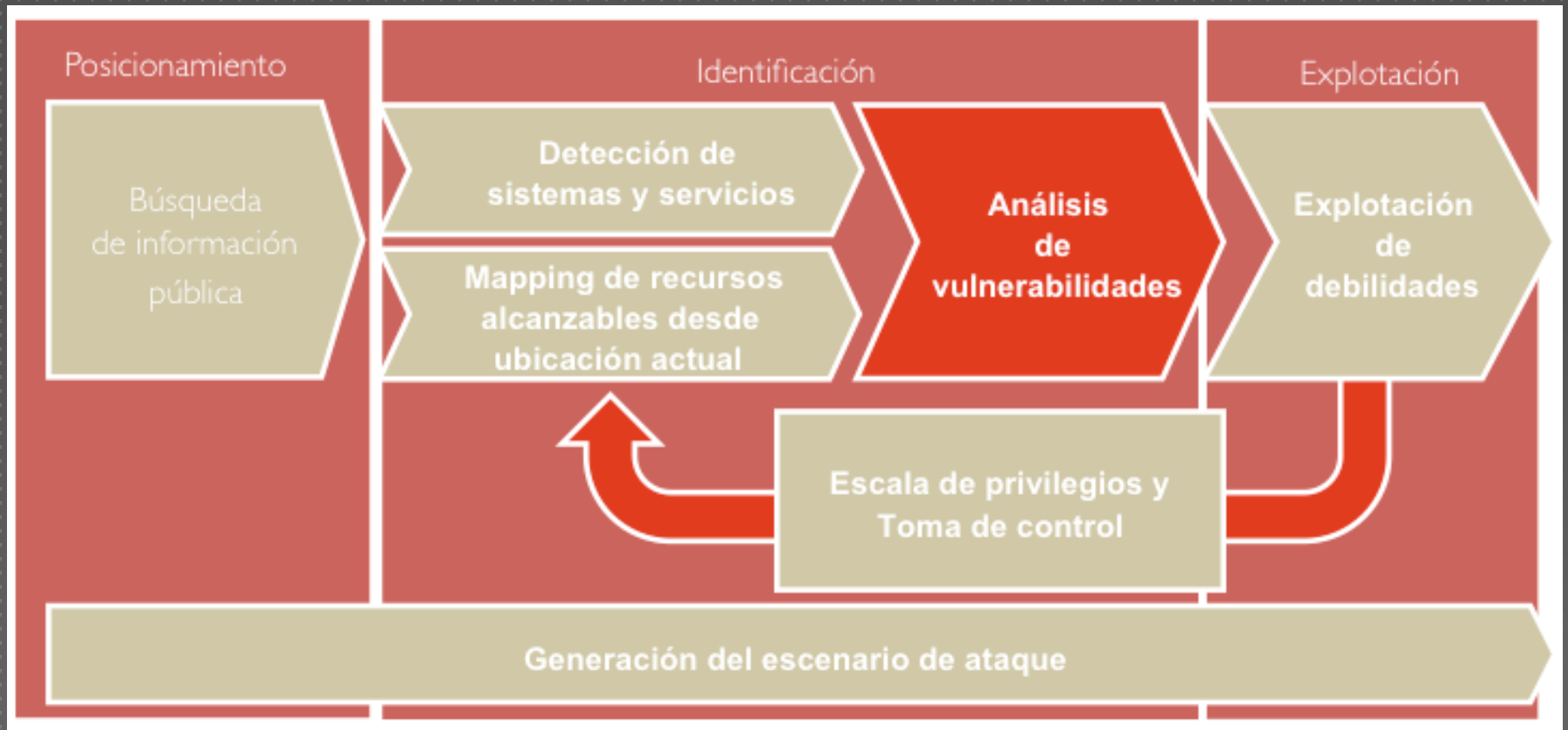
- ▶ ¿Quién soy?
- ▶ Test de intrusión “estándar”
- ▶ Recolección de credenciales y compromiso del objetivo
- ▶ Demostración
- ▶ Dudas y Preguntas

¿QUIÉN SOY?

- ▶ J. Daniel Martínez - @danIt0
- ▶ Pentester & Hacking Ético
- ▶ TigerTeam CyberSOC Deloitte
- ▶ Trabajando en IT desde los 20 años
- ▶ Alguna publicación en Blogs
- ▶ Alguna CON que otra:
 - ▶ CCN STIC
 - ▶ Navaja Negra
 - ▶ No CON Name
 - ▶ 8dot8 (Chile)
 - ▶ XIRedMasSegura



TEST DE INTRUSIÓN “ESTÁNDAR”



TEST DE INTRUSIÓN “ESTÁNDAR”

- ▶ Búsqueda de Información pública
- ▶ Localización y enumeración de servicios utilizados
- ▶ Versionado de servicios
- ▶ Búsqueda de vulnerabilidades conocidas
- ▶ Análisis en búsqueda de vulnerabilidades no conocidas (researching)
- ▶ Explotación de vulnerabilidades
- ▶ Elevación de privilegios (llegó el caos)
- ▶ Análisis de información obtenida y calculo de riesgos. Informe

TEST DE INTRUSIÓN “ESTÁNDAR”

- ▶ ¿Qué es el hacking ético? → ¿Cuál es tu equipo favorito?
- ▶ Hemos pasado un hacking ético con pocas cajas negras → ¿Prueba superada?
- ▶ Expectativa VS Realidad → Nuestra decisión

RECOLECCIÓN DE CREDENCIALES Y COMPROMISO DEL OBJETIVO

- ▶ Analizaremos la fase de Recolección de Información del Objetivo
- ▶ Hay múltiples herramientas de **extracción de direcciones de correo vía internet** usando fuentes como Google, LinkedIn, Twitter, etc. Una de las más famosas es *TheHarvester* y *Maltego*.
- ▶ Caso real: Syrian Electronic Army consigue penetrar en el periódico Washington Post a través de un ataque de **Spear Phishing**, simulando ser un remitente conocido y enviado **links de recolección de credenciales**.
 - http://articles.washingtonpost.com/2013-08-28/business/41538432_1_hackers-web-site-numerical-address
 - http://articles.washingtonpost.com/2013-08-15/lifestyle/41412289_1_electronic-army-human-rights-watch-hackers

RECOLECCIÓN DE CREDENCIALES Y COMPROMISO DEL OBJETIVO

- ▶ APT (sonido de gong)
- ▶ Es muy común que en un APT entren en juego varios vectores de ataque de forma simultánea.
- ▶ Entre los más comunes podemos destacar:
 - ❖ Intrusión interna en la compañía.
 - ❖ Spear Phishing.
 - ❖ Ataque dirigido a un empleado.
 - ❖ Mediante un USB.
 - ❖ Ataque desde el exterior a servidores e intrusión en la red interna.
- ❖ La gran mayoría de los APTs utilizan uno o varios Zero Days.
- ▶ El método estrella es atacar el eslabón más débil → Ingeniería Social



Ingeniería Social

Oficinistas, departamentos, servicio técnico... cualquier persona o grupo que permita acceder a la empresa.



0-days

Vulnerabilidades no conocidas o de alto éxito de explotación que permiten adentrarse mediante un adjunto en un email o la visita de websites fraudulentos.



Intrusiones

Intrusión en los sistemas a través de inyecciones en websites / bases de datos de la empresa publicados en Internet o Intranet, su perímetro externo

RECOLECCIÓN DE CREDENCIALES Y COMPROMISO DEL OBJETIVO

- ▶ Raspberry Pi: Mini PC con 512Mb de RAM y microprocesador ARM.
- ▶ Antena Wifi USB Alfa: AWUS036NHA Chipset Atheros.
- ▶ Batería de viaje: Batería portátil para cargar gadgets (2A).
- ▶ Debian: Distribución GNU-Linux, preparada para ejecutarse en arquitecturas tipo ARM.
- ▶ (No más de 100€)
- ▶ Tamaño Reducido



RECOLECCIÓN DE CREDENCIALES Y COMPROMISO DEL OBJETIVO

- ▶ Se creará una red WiFi con un nombre suspicaz para los empleados de la empresa del tipo “Deloitte_wifi_empleados” sin contraseña.
- ▶ Cuando un usuario se intente conectar se le pedirán las credenciales de su empresa.

Deloitte CyberSOC
http://www.apple.com
Iniciar sesión Cancelar

Deloitte.

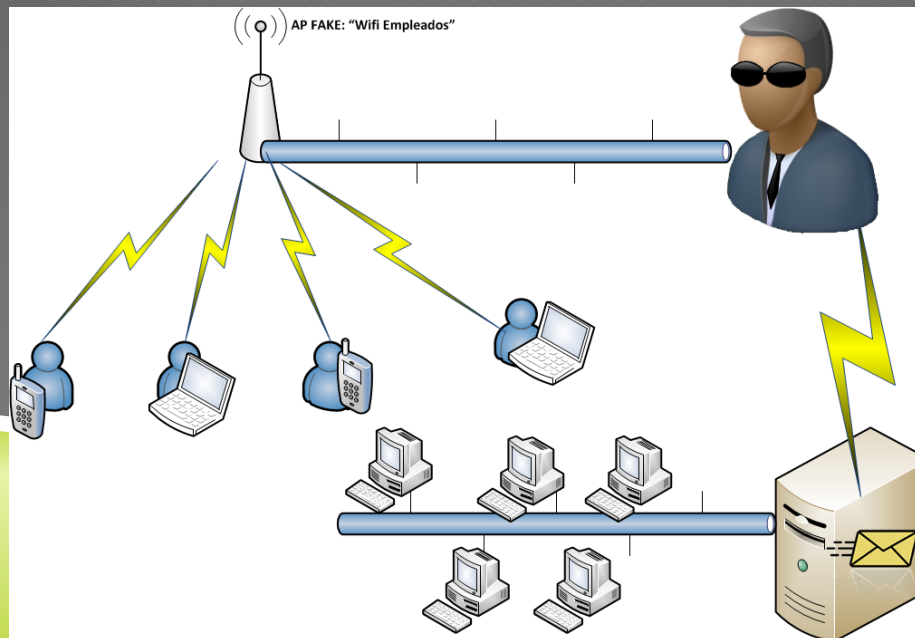
Bienvenido a la red WiFi de Deloitte para empleados
Inicie sesion para poder navegar con seguridad

Correo @deloitte.es
Password

Login

RECOLECCIÓN DE CREDENCIALES Y COMPROMISO DEL OBJETIVO

- ▶ Solo si la contraseña es válida el usuario podrá navegar de forma normal. Ésta se contrastará con algún servicio online de la **empresa objetivo**.
- ▶ Una vez obtenida la contraseña se podrá acceder al correo o cualquier otro servicio online de la empresa y se realizará un Spear Phishing dirigido con unas **probabilidades de éxito muy elevadas**.



RECOLECCIÓN DE CREDENCIALES Y COMPROMISO DEL OBJETIVO

- ▶ En nombre del usuario víctima se procederá a distribuir una campaña de *Spear Phishing* a sus contactos para proceder a la infección mediante el método elegido.
 - ❖ Ejecutable
 - ❖ Documento PDF
 - ❖ Enlace externo con exploit java, pdf, etc.
- ▶ Es suficiente que el ataque surta efecto con **un solo usuario** para que sea un **éxito**.

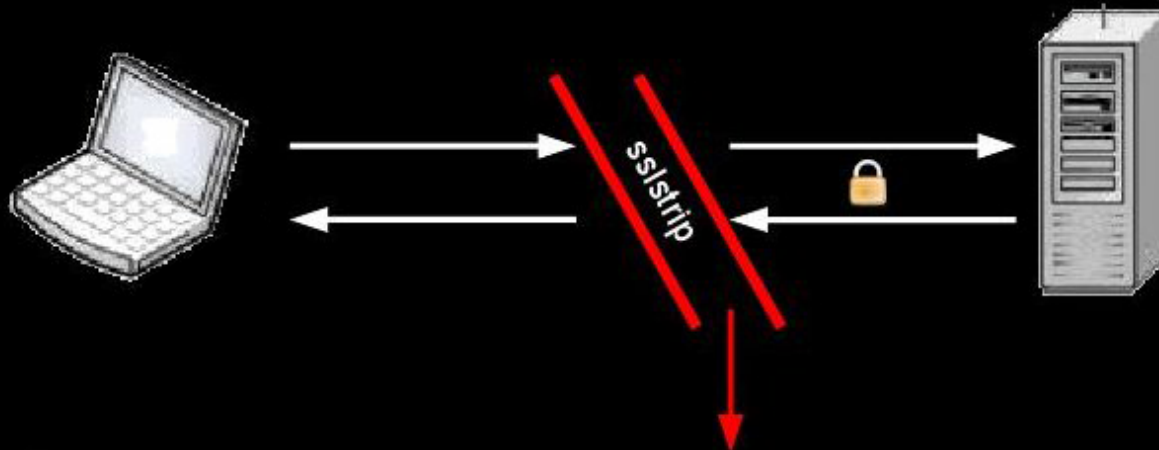


RECOLECCIÓN DE CREDENCIALES Y COMPROMISO DEL OBJETIVO

- ▶ **Interceptación de comunicaciones** de los dispositivos conectados. Tanto HTTP como SSL.
- ▶ Recolección de información sobre modelos de *smartphones*.
- ▶ **Detección de dispositivos** conectados pertenecientes al objetivo.
- ▶ Se podrían usar técnicas como **SSLstrip**
 - ❖ Mails
 - ❖ Whatapps, etc.
 - ❖ Navegación
 - ❖ Credenciales en otras plataformas.
 - ❖ En resumen: Todo el tráfico.

RECOLECCIÓN DE CREDENCIALES Y COMPROMISO DEL OBJETIVO

A First Cut Recipe: sslstrip



Watch HTTP traffic go by.

When we see an HTTP request for a URL that we've stripped, proxy that out as HTTPS to the server.

Watch the HTTPS traffic go by, log everything if we want, and keep a map of the relative links, CSS links, and JavaScript links that go by.

RECOLECCIÓN DE CREDENCIALES Y COMPROMISO DEL OBJETIVO

- ▶ Inyección *en vivo* de tráfico de red para infección de dispositivos
 - ❖ Exploits conocidos.
 - ❖ Configuraciones incorrectas (ssh iphones, desactualizaciones, jailbreaks, etc).
 - ❖ Inyección de *iframes* JavaScript.
- ▶ Funcionamiento autónomo (vía tarjeta 3G).
- ▶ Interfaz de manejo y monitoreo remoto para smartphones y tablet

DEMOSTRACIÓN: INTERFAZ

FAKE AP

DNS Bind9

ON OFF

Hostapd "Deloitte_Wifi_Empleados"

ON OFF

DHCP

ON OFF

Start All

ip Forward

ON OFF

wlan0

ON OFF

IpTables

ON OFF

Stop All

DEMOSTRACIÓN: CLIENT MONITOR

Home Client Monitor Stolen Passwords Raspberry Status

Refresh

IP Address	Auth	Product	Interface	MAC Address
192.168.1.5	YES	Apple	wlan0	b8:ff:61:71:d0:55
10.0.0.1	NO	ZyxeCom	eth0	10:7b:ef:ba:f1:08
192.168.1.48	NO	LgElectr	wlan0	8c:3a:e3:96:45:e2
10.0.0.201	NO	Apple	eth0	e4:ce:8f:20:5b:14

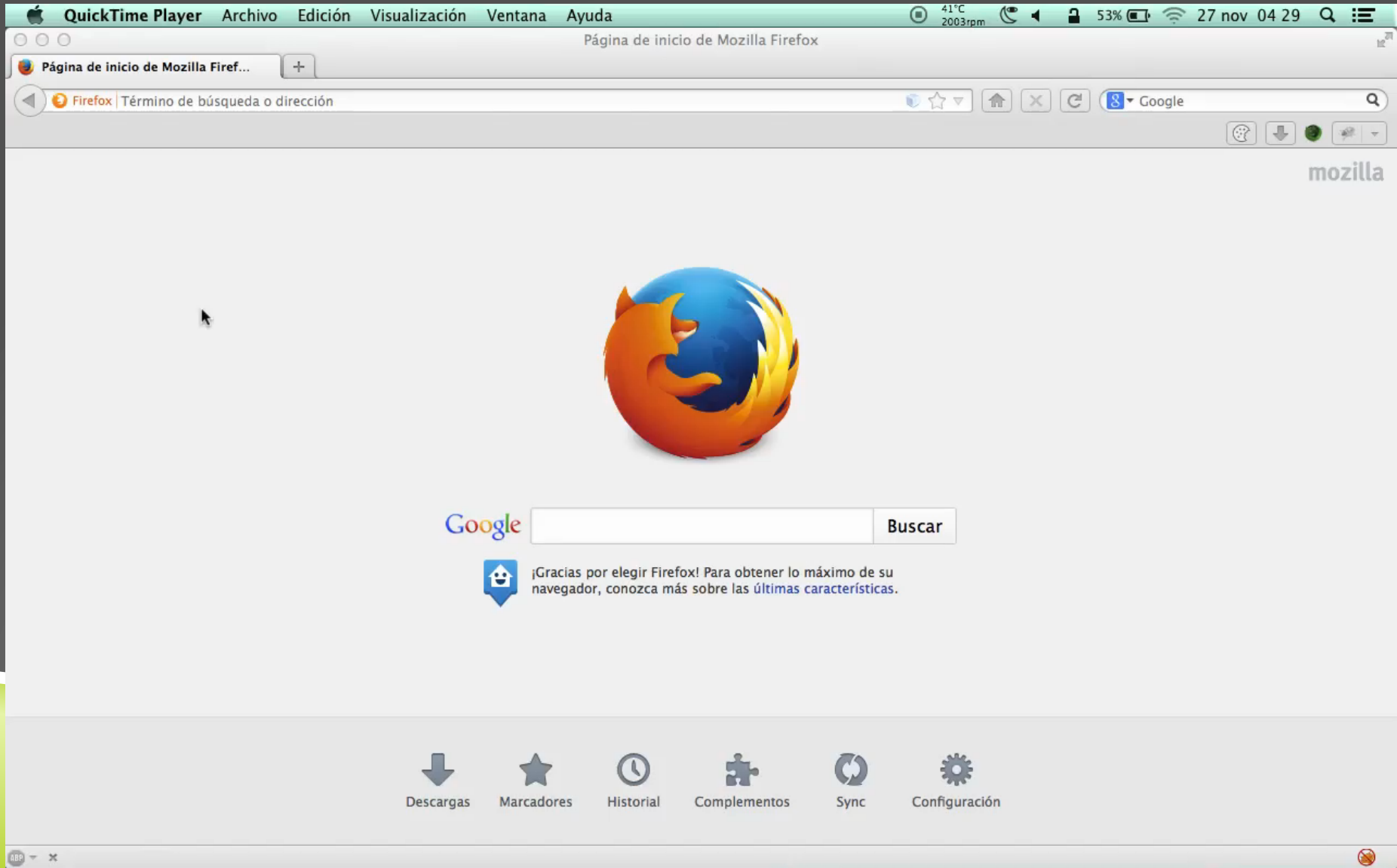
Clientes totales: 4

DEMOSTRACIÓN: PASSWORDS }:-)

Stolen Passwords:

User	Password	IP Address	MAC Adress
jmartinezcoronel@deloitte.es	Testing2013	192.168.1.4	10:68:3f:86:7f:cf
apedriza@deloitte.es	DeloitteMola	192.168.1.5	10:78:3f:86:7f:cf
jmartinezcoronel@deloitte.es	Testing2013	192.168.1.3	6c:88:14:bc:01:c8
jmartinezcoronel@deloitte.es	XXXXndola2013	192.168.1.6	b8:ff:61:71:d0:55

DEMOSTRACIÓN: CLIENT SIDE



DEMOSTRACIÓN

▶ ¿Soluciones?

- ❖ Cautela a la hora de exponer servicios empresariales
- ❖ Usar siempre VPNs
- ❖ Usar siempre certificados digitales
- ❖ Auditorias de seguridad reales
- ❖ CONCIENCIACIÓN y EDUCACIÓN

DUDAS Y PREGUNTAS

Muchas gracias por vuestra atención!

